II.

Declassified in Part - Sanitized Copy Approved for Release 2013/11/04 : CIA-RDP89B01354R000200210012-4

DEFENSE INTELLIGENCE AGENCY
WASHINGTON, D. C. 20301

13 FEB 1986

U-10,016/RS

MEMORANDUM FOR THE DEPUTY ASSISTANT SECRETARY OF DEFENSE (INTELLIGENCE) ODASD(C^3I)
ATTENTION: DIRECTOR TACTICAL INTELLIGENCE SYSTEMS

SUBJECT: Security Implications of Computers and Automated Office Equipment

Reference: ODASD(I) memorandum dated 27 January 1986, subject same as above.

1. Reference memorandum requests DIA input concerning actions being taken by TIARA elements with respect to the concerns expressed by the House Appropriations Committee. The reference requests similar inputs from the Military Departments and other DoD components. In order not to duplicate the responses of the other components involved in TIARA, this response is restricted to DIA involvement those TIARA ADP systems which are under direct control of the Tactical Intelligence Components of the DoD. DIA does have six personal computers from TIARA and projects three additional in FY86.

2. The DIA supports the operations of the Tactical Intelligence Systems in the TIARA program through provision of security policy, generic ADP programs, and review and evaluation services rather than acting as owner and operator of Tactical Intelligence ADP systems. Therefore, the DIA response is limited to issues of policy, review and evaluation, and programs in support of TIARA systems.

25X1

1 Enclosure
Tactical Intelligence and
Related Activities Rept, 1 cy (C)

Deputy Director for
Resources and Systems

ENCL 1

TACTICAL INTELLIGENCE AND RELATED ACTIVITIES

COMPUTER SECURITY

31 January 1986

PREFACE

The House Appropriations Committee requested a report on computer security for each Intelligence Community component as follows:

> "In light of the enormous resources invested in computers and automated office equipment, and the vast potential for security compromise, the Committee directs that a report be submitted by March 1, 1986 outlining the actions being taken by each Intelligence Community and Defense Department component to strengthen physical and electronic computer and automated office equipment security. In addition, the report should also specifically address changes needed in intra-office procedures to minimize security risks associated with increasingly transportable disks, tapes, etc., which may contain substantial amounts of sensitive information."

I. FOREWORD

(C) A principal objective of the U.S. Intelligence Community is to strengthen the security of intelligence activities and their operations. Measures are required to improve a full range of security needs, including those demands arising from the effects of the expanding use and increasing reliance on information systems technology. Automated word processing equipment, personal computers, minicomputers and large scale computers are providing vital and beneficial support to the Tactical Intelligence and Related Activities (TIARA). However, the combination of tremendous amounts of sensitive data being available in very concise and correlated forms in intelligence information systems, along with the fact that the systems may be subject to penetration attempts either by disloyal Americans or by foreign powers must be considered in the development and implementation of security procedures for individual offices.

II. BACKGROUND

(C) The TIARA activities have undertaken several information processing automation development and upgrade programs to support the timely collection, processing, analysis, dissemination, exchange, telecommunications and management of increasing volumes of sensitive intelligence data/information. Traditionally, TIARA activities have implemented information systems based upon Director, DIA computer security policies derived from guidance provided by NSA, the DCI and OSD governing personnel security, systems security, physical plant security and emanations from electronic equipment.

III. MANAGEMENT

(C) The Director DIA has security policy and system security accreditation policy responsibility for all Department of Defense systems which process or store Sensitive Compartmented Information (SCI). This responsibility includes systems used throughout DoD command and control, communications and tactical levels. NSA SIGINT and information systems in the CCP are under the cognizance of the Director, National Security Agency. The basic national level policies are contained in Director of Central Intelligence Directives (DCIDs) concerning protection of Intelligence Information. The Director, DIA implements those DCIDs through promulgation of Defense Intelligence Agency Directives and Manuals. As the threat and technological environment in which these information systems operate changes, these Directives and Manuals are reviewed and updated to address changes in thereat, operational, and technical environments. For example, there have already been modifications that transitioned policies and procedures from the dedicated, batch system environment through time shared teleprocessing, to the computer networking environment.

IV. STATUS

(C) Activities are underway to improve:

- Security provided for intelligence data being processed in operational systems, through retrofit of systems with security enhancements.

- Development and implementation of new technical security capabilities as standards.

- Implement the new DCI computer security safeguards and acquire future systems in accordance with DOD standards for trusted computer products.

- Security policies for the use of personal computers in GDIP activities.

A. COMPUTER SECURITY

(C) Each of the TIARA systems is evaluated for approval under the provisions of DIAM 50-4, or appropriate Military Department implementing policy, and is approved for operation by it's Designated Approving Authority. More detailed technical policy guidance such as that contained in the DCI SAFEGUARDS and the DoD Trusted Computer System Evaluation Criteria is being incorporated into the security baseline for selected critical systems as they are identified.

B. COMPUTER NETWORKING

(C) Security considerations inherent in computer networking involve control of access to system resources by individuals at remote locations and tracking (auditing and monitoring) of the activities of individuals making remote resource sharing accesses. In order to address these problems, DIA has instituted a community wide network security program called the Department of Defense Intelligence Information System (DODIIS) Network Security for Information Exchange (DNSIX). The DNSIX addresses standards, procedures and methodologies to enhance the security and controllability of intercomputer networks. The DNSIX program addresses security standards for access control, auditing, and monitoring and an ADP Security Architecture which is consistent across the community of interest. Standard devices and technologies are being centrally developed by the DIA where necessary. For example, data labeling has been included in the development of the Network Front End utilized in connecting intelligence community sites to the Defense Data Network.

C. PERSONAL COMPUTERS AND OFFICE AUTOMATION

(U) In the area of personal computers and office automation equipment, some of the principal vulnerabilities are associated with removable media, access control, hardware maintenance, software development and sharing, networking, TEMPEST, portability and auditing. Many of the currently available personal computers have little or no built in security so that these vulnerabilities must be overcome through traditional security means. In coordination with the Military Services, DIA developed and promulgated a personal computer security policy as an addendum to the basic computer

security policy manual (DIAM 50-4) for protection of intelligence information. This addendum allows limited use of such equipment either as a stand-alone system or acting as a terminal of some other computer system which is approved for the personal computer. The principal vulnerabilities are addressed in this policy which specify security guidelines and procedures for using personal computers and specifies a combination of automated and manual procedures to protect classified data/information.

D. DIRECTOR OF CENTRAL INTELLIGENCE SAFEGUARDS

(U) To carry this policy further, DIA has initiated a project with MITRE Corporation to implement and validate each of the DCI SAFEGUARDS to allow more flexible use of personal computer equipment than that allowed by the above mentioned addendum. Most of the SAFEGUARDS have been implemented and validated on a workstation under this effort. Additionally, DIA has initiated programs within DIA and the Air Force to satisfy this same set of requirements on other workstations being implemented in conjunction with specific intelligence information processing systems.

E. DIRECTOR OF CENTRAL INTELLIGENCE SECURITY COMMITTEE

(U) The DCI Security Committee (SECOM) has also provided an information booklet concerning operation of personal computer equipment when processing Intelligence Information. This booklet will be made available to users at DoD intelligence sites.

F. DOD TRUSTED COMPUTER SYSTEM PROGRAM

(U) For the future, the DoD Computer Security Evaluation Center is developing guidelines and standards, and performing research into the security improvement of commercially available products. This program will lead to off-the-shelf secure products which have been evaluated and ranked in terms of the level of security provided. It is expected that such products will include personal computing equipment in the long term.

V. TRENDS RELATED TO PERSONAL COMPUTERS

(C) The number of personal computers and word processors in the DIA portion of TIARA activity is six. The larger numbers of these systems are owned and operated by the Military Services, and will be provided by inputs from the other DoD components. Many of these computers employ paper thin floppy disk storage devices capable of holding up to 128 pages of data. The trend over the next few years will be toward doubling the number of personal computers and word processors, and increased numbers of pages per floppy disk unit. It is anticipated that the capacity of a single floppy disk will exceed 1500 pages by 1990. With the implementation of the addendum to DIAM 50-4 (enclosure 10) and standard workstation programs such as the one outlined above, the diversity of personal computers within the TIARA Community will be manageable, and controls over the movement of floppy disks and other removable storage media will be in place. However, the growth of inventories will mean that additional resources will need to be applied to administer and implement the personal computer security program.

VI. SUMMARY

(U) Word processors and small computers have little or no technical security features as part of their basic design. The risks associated with this has been balanced with the operational need to store the indicated amount of information on these systems. As part of a risk assessment, the technical security limitations of these systems have been addressed by improving administrative and procedural security measures including labeling of all storage devices and by the development of security features on the mainframe computer equipment to which many of these devices are attached. In addition, these devices are used in "closed environments" protected by those physical and personnel security techniques that traditionally have been used to protect the information processed in hardcopy form. The volume and sensitivity of information available on these devices dictates that all forms of security be employed to limit the risk while providing the processing capabilities required to satisfy operational needs.